IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF **One iPhone with IMEI number 357814437127270**	**Case No.** 22-826-ADC

AFFIDAVIT IN SUPPORT OF APPLICATIONS UNDER RULE 41
FOR WARRANTS TO SEARCH AND SEIZE

I, Michael Montevidoni, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of property—one cellular telephone—which is currently in law enforcement possession and is described in Attachment A, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and as such, am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations and make arrests for offense enumerated in Title 18, United States Code Section 2516.

3. I have been a Special Agent with ATF since 2015 and am currently assigned to the ATF Baltimore Field Division, Hyattsville Field Office, Group I. I attended the Department of Homeland Security's Criminal Investigator Training Program and ATF's Special Agent Basic

Training for a combined period of twenty-six weeks. I received extensive training in the provisions of firearms and narcotics laws administered under Titles 18, 21, and 26 of the United States Code.

4. As an ATF Special Agent, I have conducted and participated in multiple investigations concerning the illegal possession of firearms, federal controlled substance laws, and the commission of violent crimes. I have received specialized training and personally participated in various types of investigative activities, including, but not limited to: (a) the execution of search warrants; (b) the consensual monitoring and recording of conversations; and (c) the preservation of evidence.

5. I have previously participated in investigations involving illegal firearms possessions, drug trafficking, homicides, and non-fatal shootings. I have been the affiant on several search warrants and have assisted with numerous arrests. I am familiar with federal firearms and controlled substances statutes and the methods employed by those who perpetrate these crimes.

6. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The information contained in this affidavit is based upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement officers and other individuals, and analysis that others have undertaken and relayed to me. The investigation described below involves suspected violations of 18 U.S.C. § 922(i) Possession of a Stolen Firearm; (the "Subject Offense").

IDENTIFICATION OF THE PROPERTIES TO BE SEARCHED

8. The property to be searched is one iPhone with IMEI number 357814437127270 (hereinafter the "**SUBJECT PHONE**"), which law enforcement seized from **Stephawn WATSON** on January 11, 2022, in Cumberland, Maryland, as further described in Attachment A. **SUBJECT PHONE** is currently in the custody of Cumberland Police Department located at 20 Bedford Street, Cumberland, Maryland 21502 and will be taken into ATF custody on March 17, 2022.

9. The applied-for warrants would authorize the forensic examination of **SUBJECT PHONE** the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

10. On January 11, 2022 at approximately 7:45pm, City of Cumberland Police Department (CPD) officer was on patrol and observed a black Hyundai sedan bearing Virginia license plate UHJ6227 with an inoperative passenger side headlight. The CPD officer initiated a traffic stop of the aforementioned vehicle.

11. Upon approach, the CPD officer detected the strong odor of raw and burnt marijuana. The CPD officer made contact with the driver of the vehicle, who ultimately provided a false identity to avoid prosecution, but was later correctly identified as MR. The CPD officer made contact with the passenger, who identified himself incorrectly to avoid prosecution, but was later correctly identified as Stephawn WATSON. The CPD officer asked if there was anything illegal in the car, to which MR stated an excited utterance that MR and WATSON were smoking. MR provided the CPD officer with two rolled joints of suspected marijuana. The CPD

officer advised both MR and WATSON that due to the odor of marijuana and the admission of marijuana inside the vehicle, the vehicle would be searched based on that probable cause.

12. An additional CPD officer arrived on scene and assisted in search of the vehicle. The CPD officer located a handgun, later identified as a Taurus, 9mm pistol bearing serial number TMR88351 and loaded with 16 rounds of ammunition, under the passenger front seat of the vehicle, in the immediate possession and span of control of WATSON. Further, a search incident to arrest revealed an additional amount of marijuana located on WATSON's person. CPD officers located WATSON's true Maryland identity in the pocket behind the passenger seat as well.

13. A check of the Taurus 9mm pistol bearing serial number TMR88351 revealed that the aforementioned firearm was stolen out of Hampton, Virginia on or about September 15, 2020. The owner of the firearm was contacted, and she confirmed the item had been stolen out of her vehicle, that she reported this to the police, and that she does not know WATSON nor did he have permission to be in possession of her firearm.

14. CPD officers read MR and WATSON their Miranda Rights. WATSON declined to speak with CPD Officer(s). MR agreed to speak with CPD officer(s). MR stated that she did not know that WATSON was in possession of the stolen firearm and she did not know that the firearm was in the vehicle.

15. CPD officers were also made aware that MR and WATSON currently had active arrest warrants. Both were arrested and transported to central booking.

16. Your affiant is aware the WATSON, at the time of his arrest by CPD, was currently under indictment from August 11, 2020, from the Prince George's County Circuit Court for charges of ILLEGAL POSSESSION OF A REGULATED FIREARM and WEAR

AND CARRY A LOADED HANDGUN, and related charges. WATSON failed to appear for his trial date in this matter on November 29, 2021, and a bench warrant was issued for his arrest.

17. **ADDITIONAL INFORMATION RELATED TO SEARCHES OF THE DEVICE**

18. On numerous occasions, your affiant and other law enforcement officers have observed WATSON holding and displaying firearms in photographs and posts to social media, often including violent messages and threats. These photographs were posted to social media during the months of January of 2021 and November, October, and September of 2020, when WATSON was prohibited from possessing firearms for being under indictment.

19. Based on my knowledge, training, and experience, as well as my experience with other investigations and search warrants, with respect to **SUBJECT PHONE**, such evidence includes photographs and videos that show prohibited individuals with the possession of firearms, to include stolen firearms. These photographs and videos are typically stored within the cell phone. Photographs and videos, and their associated information, can provide evidence of the illegal possession or criminal acts and potential locations at times relevant to the investigation, as well as documentation of the commission of the Subject Offenses.

20. I know, based on my training, experience, and participation in this and other investigations that individuals involved with illegal firearm possession frequently use cell phones and social media to further their illegal activities. Specifically, I know that:

a. Persons who illegally possess firearms tend to use their cell phones to take photographs or videos depicting those items, which are uploaded and stored in their phone storage, as well as their social media accounts. As to Instagram in particular, individuals can make "stories" featuring those same photographs or videos.

b. Not only do suspects frequently use those social media accounts to post photographs or videos of the firearms, but they also post images of themselves with those items, comment on images of themselves with those items, or are tagged in such photographs or videos posted by others. These accounts also include other valuable evidence linking the suspects to criminal activity, like images showing them in the area of a crime (including an arrest for prohibited possession of those items or a discharging, shooting, or homicide) at the time it occurred, wearing clothes matching those of a known suspect, having possession of other tools or instrumentalities at another time, or other identifying or relevant information.

c. Persons who possess firearms (including stolen firearms), illegally use their social media accounts to communicate with others in reference to the possession, purchase, selling, transfer, or intended use of those items. Social media platforms allow users to communicate with one another via private messages or post comments to photographs and videos that are accessible to a wider audience consisting of the user's "friends" or "followers" or the public. This can include by "tagging" people in their posts or adding "hashtags" or other text, which tags and hashtags can refer explicitly to criminal organizations. Records of these communications, including the communications themselves (if not deleted by the social media user), are often stored by the relevant social media platform for extended periods of time.

21. I know through my training and experience that subjects will use cellular phones, which can be connected wirelessly to the Internet, before, during and after the commission of crimes, to plan the commission of the criminal acts, and to communicate to any subjects assisting

in the criminal act, such as the act of stealing firearms or possessing stolen firearms. The electronically stored information on cellular telephones is of evidentiary value in identifying potential other members of the criminal acts and establishing the relationship between these individuals, as well as in confirming the course of criminal schemes. Those involved in criminal acts may also record photographs and videos of the locations of the firearms theft, as well as run Internet search terms related to the location(s) involved, in the time leading up to the theft. Internet search terms and other information stored on cellular telephones, can also include metadata and geographic location data.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email, including through a variety of applications, or "apps;" taking, sending, receiving, and storing still photographs and moving video in a manner akin to a digital camera; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones

may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the global positioning system to display its current location. It often records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The global positioning system (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four

numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that **SUBJECT PHONE** has capabilities that allow them to serve as wireless telephones, digital cameras, and GPS navigation devices, *e.g.*, and to store extensive data. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, as well as evidence of crimes under investigation.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices such as cellular telephones and SIM cards can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on cellular telephones, and subscriber is stored on SIM cards. This information can sometimes be recovered with forensics tools.

a. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded

onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer or other electronic device, such as a cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's or cellular telephone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the Subject Offenses, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on **SUBJECT PHONE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit the examination of **SUBJECT PHONE** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because the warrants seek only permission to examine devices already in law enforcement's possession, the execution of these warrants does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for search warrants authorizing the examination of **SUBJECT PHONE** described in Attachment A to seek the items described in Attachment B, which are evidence, fruits, and instrumentalities of the Subject Offenses.

Respectfully submitted,

Michael Montevidoni
Special Agent
Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 15th day of March, 2022.

A. David Copperthite

A. DAVID COPPERTHITE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is one iPhone with IMEI number 357814437127270, hereinafter the "**SUBJECT PHONE**." **SUBJECT PHONE** is currently in the custody of Cumberland Police Department located at 20 Bedford Street, Cumberland, Maryland 21502 and will be taken into ATF custody on March 17, 2022.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on **SUBJECT PHONE** described in Attachment A and relating to violations of 18 U.S.C. § 922(n) Possession of a Firearm by a Prohibited Person/Person Under Indictment and 18 U.S.C. § 922(i) Possession of a Stolen Firearm (the "Subject Offenses"), and evidence, contraband, fruits, or instrumentalities of such violations committed by persons known and unknown, including:

a. Images of firearms;

b. Records and information concerning firearms, controlled substances, and the purchase, sale, and/or transfer of firearms;

c. Documents and records showing email and telephone contacts and numbers called, such as SIM cards, address books, call histories, and telephone bills;

d. Photographs and/or videos, in particular photographs and/or videos of potential co-conspirators and their criminal associates, assets, and/or criminal activities, and associated geographical location, related to the Subject Offense;

e. Documents and records indicating travel in interstate and foreign commerce, such as travel itineraries, rental car records, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, telephone bills, Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, or origination points;

f. Records of browsing history, Internet searches, search terms, and search results, and associated geographic location, related to the Subject Offense;

g. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone

numbers dialed from the Device and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

h. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the Subject Offense;

i. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted;

j. Evidence indicating the device user's state of mind as it relates to the Subject Offense;

k. Evidence of the attachment to Device of other storage devices or similar containers for electronic evidence;

l. Evidence of the times the Device was used;

m. Passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the Device;

n. Records of or information about Internet Protocol addresses used by the Device;

o. Records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

p. Contextual information necessary to understand the evidence described in this attachment.

q. Any and all evidence, records, or information of firearms and ammunition possession.

r. Any and all evidence, records, or information pertaining to financial proceeds from or because of firearms.

2. The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possibly recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

f. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file, or storage area shall cease.

With respect to the search of all information obtained pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the Court. The investigative team may continue to review any information not segregated as potentially privileged.